Waingels School ICT and internet Acceptable Use Policy

Better Never Stops

Next review due by:	Jan 2024

Contents

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

> Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors

> Establish clear expectations for the way all members of the school community engage with each other online

> Support the School's policy on data protection, online safety and safeguarding

> Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems

> Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our School's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy and code of conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

> Data Protection Act 2018

> The General Data Protection Regulation

> Computer Misuse Act 1990

> Human Rights Act 1998

> The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

> Education Act 2011

> Freedom of Information Act 2000

> The Education and Inspections Act 2006

> Keeping Children Safe in Education 2018

> Searching, screening and confiscation: advice for schools

3. Definitions

> **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

> **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

> **"Personal use":** any use or activity not directly related to the users' employment, study or purpose

> **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

> **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the School's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the School's ICT facilities includes:

> Using the School's ICT facilities to breach intellectual property rights or copyright

> Using the School's ICT facilities to bully or harass someone else, or to promote unlawful discrimination

> Breaching the School's policies or procedures

> Any illegal conduct, or statements which are deemed to be advocating illegal activity

> Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

> Activity which defames or disparages the school, or risks bringing the school into disrepute

> Sharing confidential information about the school, its pupils, or other members of the school community

> Connecting any device to the School's ICT network without approval from authorised personnel

> Setting up any software, applications or web services on the School's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data

> Attempt to install any software on any school computer or alter the configuration of existing software

> Attempt to bypass the AUP required to be accepted in order to use a PC Attempt to monitor the Waingels network using network monitoring software

> Attempt to access passwords, system utilities, product keys, command line utilities, view or edit the registry of a machine, access UNC shares.

> Search for Network Management Software or Hardware, including virtual server infrastructures.

> Attempt to access areas of our network that are not part of the standard software installed to PC's or mapped network drives available to students.

> Use, send or access abusive or offensive language, pictures or other material.

> Bring into school any removable media, such as USB drive, containing any offensive or abusive material.

> Use or access auction sites, such as eBay, without permission unless in conjunction with school business.

> Purchase goods or use credit/debit cards over the school network.

> Download executables (.exe), zip (.zip), mp3 (.mp3) files from the Internet, E- Mail or personal storage devices without direct permission from a member of staff.

> Use the internet to send SMS/texts.

> Disconnect peripherals (such as headphones or mouse) or otherwise alter the physical configuration of a workstation.

> Connect a digital music player, PDA or other digital storage device including mobile phones to a school computer or school network without permission from a member of the staff.

> Store illegally copied music files on any part of the school system.

> The school internet facilities are not for personal or non-school-related use.

> Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

> Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the School's ICT facilities

- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the School's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher or any other relevant member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the School's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. This can be requested by initially emailing supportdesk@waingels.wokingham.sch.uk who will then pass on the matter to the relevant member of SLT for consideration.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the School's policies on discipline, code of conduct and culture and values.

Unacceptable ICT use may result in a user's access/permissions been revoked indefinitely.

Policies can be found on the resources area of the school network or requested from ITsupport@waingels.wokingham.sch.uk

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The School's IT Support team manages access to the School's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the School's ICT facilities.

Staff who need their access permissions updated or changed, should contact the IT Support team on extension 2251 or email supportdesk@waingels.wokingham.sch.uk .

This may also need subsequent approval from SLT before being actioned

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

When sending emails that contain personal data they should be sent 'secure'. The word 'secure' must be included in square brackets in the subject line. [SECURE] This works for all external email addresses and forces the recipient to setup a password to retrieve the email. The recipient only has to do this once and then every time they are sent an email from this establishment they can only view it by entering the password. It is not required for internal email. If you are unsure, please ask the ICT support team for help.

You can password protect files but if you are sending them via email you have to send the password by another method – not another email. If you are unsure, please ask the ICT support team for help.

Personal data" includes names, addresses, phone numbers and IP addresses, as well as what GDPR calls "factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". That includes biometrics such as face, fingerprint and iris recognition, and genetic information. In other words, you may have personal data that identifies someone even if you don't know their name. Caution should be exercised when sending confidential information via e-mail.

The transmission of confidential information via e-mail to unauthorised persons is strictly prohibited

The use of e-mail for personal purposes is permitted but must be reasonable

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the school Business Manager and Data Protection Office immediately and with their guidance follow our data breach procedure. Email address dpo@waingels.wokingham.sch.uk extension 2232

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The School Business Manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

> Does not take place during contact time with students/teaching hours/non-break time

> Does not constitute 'unacceptable use', as defined in section 4

> Takes place when no pupils are present

> Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the School's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the School's ICT facilities for personal use may put personal communications within the scope of the School's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the School's ICT and internet acceptable use policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the School's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the School's ICT facilities and materials remotely.

This is accessed using a secure portal https://remote.waingels.wokingham.sch.uk

> It is managed by the IT support team supportdesk@waingels.wokingham.sch.uk

> On first use It requires you to install a small application on your personal devices that checks if your software and hardware are safe. This software communicates with the remote access system and will determine if your device has an up to date windows system and antivirus. Access is granted to our network dependent on the above criteria.

> The remote access system does not allow saving to your personal devices at home. If you want to use/take work off site you must use an encrypted memory stick which is provided by the school or your laptop must be encrypted. All staff provided laptops are BitLocker encrypted.

> All staff are provided with a Microsoft Office 365 account and a Google Account. Which provides access to Microsoft One drive personal storage area, Google Classroom and Google Drive. These locations are encrypted by their vendor and therefore it is safe to store work related files and personal school related documents in these locations and access them both internally and externally. Thought and care must be taken with the content of what you store and what devices you use to access these locations. If you download school related files and documents to your personal devices it is your responsibility to ensure that your devices are safe and encrypted,

Staff accessing the School's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the School's ICT facilities outside the school and take such precautions against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our policies and in particular the data protection policy.

The schools data protection policy is on the school website under policies

5.4 School social media accounts

The school has various social pages on Twitter, Facebook, Instagram, LinkedIn and YouTube overseen by Melissa Yiannapas. Staff members who have not been authorised to manage, or post to these accounts, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines according the Waingels social media policy which can be found https://www.waingels.wokingham.sch.uk/243/policies-1 .

5.5 Monitoring of school network and use of ICT facilities

All devices are monitored with software for safeguarding purposes.

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

> Internet sites visited

> Bandwidth usage

> Email accounts

> Telephone calls

> User activity/access logs

> Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

> Obtain information related to school business

> Investigate compliance with school policies, procedures and standards

> Ensure effective school and ICT operation

> Conduct training or quality control exercises

> Prevent or detect crime

> Safeguarding

> Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1 Access to ICT facilities

Explain which ICT facilities are available to pupils, when and under what circumstances. For example:

> "Computers and equipment in the School's ICT suite are available to pupils only under the supervision of staff"

> "Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff"

> "Pupils will be provided with an account linked to the School's and several virtual learning environments, like office365, Google Classroom, Show My Home Work and others which they can access from any devices

> "Sixth-form pupils can use the computers independently for educational purposes only"

> Sixth form can bring their own device to school and connect to the BYOD student wireless. This will allow them filtered and monitored internet access as well as the ability to connect to a virtual desktop using the remote access systems.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the School's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the culture and values policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

> Using ICT or the internet to breach intellectual property rights or copyright

> Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination

> Breaching the School's policies or procedures

> Any illegal conduct, or statements which are deemed to be advocating illegal activity

> Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

> Activity which defames or disparages the school, or risks bringing the school into disrepute

> Sharing confidential information about the school, other pupils, or other members of the school community

> Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel

> Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the School's ICT facilities

> Causing intentional damage to ICT facilities or materials

> Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

> Using inappropriate or offensive language

Sanctions will apply if pupils do or attempt to do any of the above. They will be disciplined in line with the schools culture and values policy and acceptable ICT use. In serious cases, this may include permanent exclusion.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the School's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the School's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the School's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the School's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information will face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Passwords for staff

Passwords must have a minimum length of 8 characters

Passwords must have a minimum age of 1 day and a maximum age of 180 days

Password history is enforced to not allow the last two passwords used when updating your password.

Password must meet Microsoft minimum complexity rules which are:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
    English uppercase characters (A through Z)

    English lowercase characters (a through z)

    Base 10 digits (0 through 9)

    Non-alphabetic characters (for example, !, $, #, %)

Also, it has been agreed that passwords must be changed at the start of each school year in September. Therefore, the IT systems will force a password update at login prior to term starting in the first week of September 2019.

Passwords for Pupils

Passwords must have a minimum length of 8 characters

8.2 Software updates, firewalls, and anti-virus software

All of the School's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the School's ICT facilities.

Any personal devices using the School's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the School's data protection policy.

The School's data protection policy can be found on the schools website under policies.

8.4 Access to facilities and materials

All users of the School's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the schools IT Network Manager.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them,

they should alert IT support and the data protection officer supportdesk@waingels.wokingham.sch.uk extension 2251 and dpo@waingels.wokingham.sch.uk extension 2230 immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day unless instructed otherwise.

To lock a PC quickly press the windows key and the L key together. Or press control alt delete and select the lock option.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption

9. Internet access

The school wireless internet connection is secured.

> The school using SEGFL safety net plus User based filtering systems.

> This has separate connections for staff/pupils/parents and the public

Your internet access goes through a user-based filtering system and records the websites you have visited

9.1 Pupils

> The schools Wi-Fi is for 6th form access, staff and Guest access only. If you are a pupil between years 7 and 11 unless given explicit permission by staff, you are not allowed to connected to schools Wi-Fi using a personal device

> The school uses radius authentication for wireless and an internet filtering and monitoring system for personal devices.

> Allowed pupils can authenticate to the student wireless SSID Wi-Fi beacon and authenticate with their school username and password. If access is not granted please report this to supportdesk@waingels.wokingham.sch.uk, telephone extension 2251

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the School's Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

> Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

> Visitors need to access the School's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Visitors and parents can request access at reception. They will be provided with a token or username and password to authenticate. This will allow them business hours access 9-5 or after hours if requested and approved by the school.

10. Monitoring and review

The headteacher and Network Manager, School Business Manager and SLT monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed biannually.

11. Related policies

This policy should be read alongside the School's policies on:

- Online safety
- Culture and Values
- Code of Conduct
- Disciplinary
- Data protection

Appendix 1: Facebook cheat sheet for staff

<div style="border: 2px solid magenta; padding: 20px;">

Don't accept friend requests from pupils on social media

</div>

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

> Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

> Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

> The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

> **Google your name** to see what information about you is visible to the public

> Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

> Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

> In the first instance, ignore and delete the request. Block the pupil from viewing your profile

> Check your privacy settings again, and consider changing your display name or profile picture

> If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

> Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

> It is at your discretion whether to respond. Bear in mind that:

  • Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

  • Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

> If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

> **Do not** retaliate or respond in any way

> Save evidence of any abuse by taking screenshots and recording the time and date it occurred

> Report the material to Facebook or the relevant social network and ask them to remove it

> If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

> If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

> If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Facebook page • Email/text groups for parents (for school announcements and information) • Our virtual learning platform Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the School's official channels, so they can be dealt with in line with the School's complaints procedure I will not: • Use private groups, the School's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the School's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the School's ICT facilities and internet: agreement for pupils and parents/carers
When using the School's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the School's network using someone else's details • Bully other people I understand that the school will monitor the websites I visit and my use of the School's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the School's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the School's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the School's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the School's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the School's network
- Share my password with others or log in to the School's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the School's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the School's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the School's ICT systems and internet responsibly, and ensure that pupils in my care do so too.